



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,797	05/22/2001	Thomas L. Gindin	POU920010018US1	1174

7590 06/03/2005

Sean F. Sullivan  
Cantor Colburn LLP  
55 Griffin Road South  
Bloomfield, CT 06002

EXAMINER
----------

SON, LINH L D

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 06/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/862,797

Applicant(s)

GINDIN ET AL.

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 22 May 2001.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. This office action is responding to the amendment received on 03/15/05.
2. Claims 1, 8 and 15 are amended.
3. Claims 22-24 are newly added.
4. Claims 1-24 are pending.

### ***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benantar, US Publication No. 20020144108A1, hereinafter '108.

7. As per claims 1, 8, 15, and 22-24, "a method for creating a proof of possession confirmation for inclusion by a certification authority into a digital certificate, the digital certificate for use by an end user, the method comprising: receiving, from the certification authority in response to a certificate request by the end user, a plurality of data fields corresponding to a target host system, the identity of the end user, and a proof of identity possession by the end user" is taught in '108 (Para 0060, 0061, 0075, and 0078, and 0044 (Public Key is the proof of identity possession)); "analyzing the

content of said plurality of data fields; verifying the accuracy of said plurality of data fields; and if said plurality of data fields is verified as accurate, sending a signed object to the certification authority, said signed object comprising the proof of possession confirmation” is taught in ‘108 (Para 0083-0086). However, Benantar is silent on the limitation “said proof of possession confirmation is constructed in a manner so as to prevent replay attacks by an imposter”. Nevertheless, Benantar teaches of forming the authenticate data comprises of numbers of information in (Para 0075). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify the invention to incorporate a onetime use piece of data for one time access to prevent replay attacks by an imposter and further increasing security measure to the system.

8. As per claims 2, 9, and 16, “the method of claims 1, 8, and 15, wherein said plurality of data fields further comprises: a host name; a subject identification; a subject public key information; and a sealed proof of possession” is taught in ‘108 (Para 0075, and 0078).

9. As per claims 3, 10, and 17, “the method of claims 2, 9, and 16, wherein analyzing the content of said plurality of data fields further comprises: decrypting a proof of possession structure from said sealed proof of possession; extracting a password from said sealed proof of possession structure; extracting a key identifier from said proof of possession structure; and calculating a correct key identifier from said subject

public key information" is taught in '108 (Para 0075, and 0078-0080).

10. As per claims 4, 11, and 18, "the method of claims 3, 10, and 18, wherein the accuracy of said plurality of data fields is verified if: said host name is matched with an identity of said target host system; said extracted password is validated as a valid password for the end user; and said extracted key identifier is matched with said correct key identifier calculated from said subject public key information" is taught in '108 (Para 0077-80).

11. As per claims 7, 14, and 21, "the method of claims 1 and 8, wherein: said plurality of data fields includes a password; and said signed object does not include said password" is taught in '108 (Para 0075, and Fig. 5, 516).

12. As per claims 5-6, 12-13, and 19-20, "the method of claims 3 and 10, wherein said extracted password and said extracted key identifier are initially symmetrically encrypted" is taught in '108 (Para 0089). It is well know in the art that the X.509 certificate utilizes symmetrical and asymmetrical encryption utilizing private-public key.

***Response to Amendment***

13. Applicant has amended the independent claims 1, 8, and 15, which necessitated new grounds of rejection. See Rejections above.

***Conclusion***

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

**Conclusion**

15. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-272-3856.


Art Unit: 2135

16. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

17. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see <http://pzr-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

**Linh LD Son**

**Patent Examiner**

  
Primary Examiner  
AU 2135